UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE
MEMPHIS DIVISION

EVIN SHEFA, individually and on behalf of all others similarly situated, Plaintiff, v. EVOLVE BANK & TRUST and YOTTA TECHNOLOGIES, INC., Defendants.	Case No. **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Evin Shefa ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through the undersigned attorneys, brings this Class Action Complaint against Defendants Evolve Bank & Trust ("Evolve Bank") and Yotta Technologies, Inc. ("Yotta" and, with Evolve Bank, "Defendants"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters as follows.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard Plaintiff's and Class members' personally identifiable information ("PII"), including names, Social Security numbers, bank account numbers, and contact information.

2. Evolve Bank is a financial company that operates as both a personal bank and provides banking services to financial technology companies and other companies for end users. Evolve Bank provides these services to Yotta. Yotta is a financial technology company that provides lottery savings accounts to consumers, in which consumers can deposit money into

accounts that will then be used for lottery drawings. The financial accounts are maintained by Evolve Bank.

3. In or about late May 2024, Evolve Bank experienced a ransomware attack on its network systems, which resulted in hackers accessing and downloading the PII of Plaintiff and Class members and leaking the PII on the dark web (the "Data Breach"). Evolve Bank has revealed that the Data Breach affected approximately 7,640,112 persons.

4. Defendants promised Plaintiff and Class members that they, or the third parties they contract and share PII with, would implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class members' PII against unauthorized access and disclosure. Defendants breached those promises by, *inter alia*, failing to, or sharing PII with third parties who failed to, implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, unjust enrichment, violation of the California Consumer Protection Act of 2018, and violation of the California Unfair Competition Law, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Evin Shefa

7. Plaintiff Evin Shefa is a citizen and resident of California.

8. Plaintiff is a customer of Yotta. As a condition of receiving services from Yotta, Yotta required Plaintiff to provide it with his PII. By using Yotta's services, Plaintiff's PII was also given to Evolve Bank.

9. Plaintiff believed that Yotta had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff provided his PII to Yotta in exchange for receiving services from Defendants.

10. In connection with providing services to Plaintiff, Defendants collected, stored, shared, and maintained Plaintiff's PII on their systems, including the systems involved in the Data Breach.

11. Had Plaintiff known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Defendants with his PII or obtained services from Defendants.

12. On July 30, 2024, Plaintiff received an email from Evolve notifying him that his PII was exposed in the Data Breach.

13. As a result of the Data Breach, Plaintiff has purchased LifeLock to monitor for identity theft, paying $15 per month for the service.

14. Since the Data Breach, Plaintiff has noticed a significant increase in the number of spam emails and text messages.

15. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and

loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendant Evolve Bank & Trust

16. Defendant Evolve Bank & Trust is an Arkansas corporation with its headquarters located at Triad Centre I, 6000 Poplar Avenue, Suite 300, Memphis, Tennessee 38119.

Defendant Yotta Technologies, Inc.

17. Defendant Yotta Technologies, Inc. is a Delaware corporation with its headquarters located at 33 Irving Pl., New York, NY 10003.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has general personal jurisdiction over Defendant Evolve Bank because it is a corporation that maintains its principal places of business in this State, regularly conducts business in this State, and has sufficient minimum contacts in this State.

20. This Court has personal jurisdiction over Defendant Yotta because it regularly conducts business in this State, contracts to supply goods or services in this State, has sufficient minimum contacts in this State, and contracts with Evolve Bank.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Evolve Bank's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

22. Evolve Bank is a financial services institution that provides personal banking, open banking, and mortgage lending services.[1] The company claims to be "a global leader in the payments and BaaS industry" and provides banking services to individuals and small businesses through online banking.[2]

23. Yotta is an online platform that allows consumers to create savings accounts and enter the users into daily lottery drawings with the number of tickets based on the amount of funds in the account.[3]

24. Yotta's website notes that, in addition to submitting their name, email address, and phone number to make an account, in order to open a savings account and participate in daily prize draws, customers need to submit their "address, date of birth, and social security number."[4]

25. Yotta's website contains a privacy policy, which states, "Yotta is committed to maintaining the confidentiality, integrity and security of any personal information about our users."[5] The privacy policy also states that "The security of your personal information is important to us."[6]

---

[1] *Home*, Evolve Bank, https://www.getevolved.com/ (last accessed Aug. 6, 2024).
[2] *Beyond Banking Investor Relations 2024*, Evolve Bank, https://www.getevolved.com/wp-content/uploads/2024/03/Investor-Kit-2024_v03-25-24.pdf (last accessed Aug. 6, 2024).
[3] *Yotta review 2023*, moneywise, https://moneywise.com/banking/banking-reviews/yotta-review (last accessed Aug. 6, 2024).
[4] *What information do I provide in order to sign up?*,Yotta, https://help.withyotta.com/en/articles/4495118-what-information-do-i-provide-in-order-to-sign-up (last accessed Aug. 6, 2024).
[5] *Privacy Policy*, Yotta, https://www.withyotta.com/privacy (last accessed Aug. 6, 2024).
[6] *Id*.

26. Evolve Bank's website also contains a consumer privacy policy, which states, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."[7]

27. Plaintiff and Class members are, or were, customers of Evolve Bank, Yotta, or both, and entrusted Defendants with their PII.

The Data Breach

28. In or about late May 2024, Evolve Bank determined that an unauthorized person had accessed its network systems.[8] Upon further investigation, Evolve Bank determined that the intrusion was a ransomware attack and that the ransomware group, LockBit, had downloaded customer PII, including "names, Social Security numbers, bank account numbers, and contact information."[9]

29. After Evolve Bank refused to pay the ransom, LockBit released the files containing the PII of Plaintiff and Class members onto the dark web.[10]

30. While Evolve Bank discovered the Data Breach in or about late May, 2024, Defendants did not begin to notify impacted breach victims about the Data Breach until approximately July 8, 2024, over a month after the Data Breach was discovered.[11] Defendants' failure to promptly notify Plaintiff and Class members that their PII was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could

[7] *Consumer Privacy Policy Notice*, Evolve Bank, https://www.getevolved.com/wp-content/uploads/2023/03/Evolve-Consumer-Privacy-Policy-Notice-12-22-Final.pdf (last accessed Aug. 6, 2024).
[8] *Cybersecurity Incident*, Evolve Bank, https://www.getevolved.com/about/news/cybersecurity-incident/ (last accessed Aug. 6, 2024).
[9] *Id*.
[10] *Id*.
[11] *Id*.

monetize, misuse, or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their PII will be misused and their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII

31. At all relevant times, Defendants knew, or should have known, that the PII they collect, share, and maintain was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from unauthorized access that Defendants should have anticipated and guarded against.

32. It is well known among companies that store sensitive personally identifying information that such information—such as the PII stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[12]

33. PII is a valuable property right.[13] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent

[12] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[13] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[14] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY

over $19 billion on acquiring personal data of consumers in 2018.[15] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

34. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security Numbers, PII, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

35. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[16]

36. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

(Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[15] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[16] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII Has Grave and Lasting Consequences for Victims

37. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[17] [18]

38. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[19]

39. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[20]

40. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

---

[17] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Aug. 6, 2024).

[18] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[19] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[20] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Aug. 6, 2024).

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[21]

41. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

42. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased and imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

43. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

44. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

[21] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

> All persons whose personally identifiable information was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

45. Plaintiff also brings this action on behalf of himself and all members of the following Subclass of similarly situated persons (the "Yotta Subclass"):

> All persons whose personally identifiable information was provided to Yotta and was accessed in the Data Breach by unauthorized persons, including all such persons who were sent a notice of the Data Breach.

46. Excluded from the Class are Evolve Bank & Trust, and its affiliates, parents, subsidiaries, officers, agents, and directors, and Yotta Technologies, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

47. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

48. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Evolve Bank reported to the Office of the Maine Attorney General that 7,640,112 persons were affected by the Data Breach.[22]

49. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;

[22] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a2e61e38-f78d-403d-9abb-3810771bb5d2.html (last accessed Aug. 6, 2024).

b. whether Defendants had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

c. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

d. whether an implied contract existed between Class members and Yotta, providing that Yotta would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

e. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;

f. whether Defendants breached their duties to protect Plaintiff's and Class members' PII; and

g. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

50. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and all other Class members. Individual questions, if any, pale in comparison in both quantity and quality to the numerous common questions that dominate this action.

51. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

52. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature. Plaintiff has no interests adverse to, or

that conflict with, the Class he seeks to represent. Plaintiff and his counsel have adequate resources to assure the interests of the Class will be adequately represented.

53. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

54. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

55. Defendants owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting the PII in their possession, custody, or control.

56. Defendants knew, or should have known, the risks of collecting, sharing, and storing Plaintiff's and Class members' PII, and the importance of maintaining secure systems. Defendants knew, or should have known, of the many data breaches that targeted companies storing PII in recent years.

57. Given the nature of Defendants' business, the sensitivity and value of the PII they collect, share, and maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

58. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

59. It was, or should have been, reasonably foreseeable to Defendants that their failure to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

60. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

61. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to

compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

62. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

63. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

64. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

65. Defendants' violations of Section 5 of the FTCA constitute negligence per se.

66. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA were intended to protect.

67. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA were intended to guard against.

68. It was, or should have been, reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

69. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT
Against Yotta

70. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

71. Plaintiff brings this claim individually, and on behalf of the Yotta Subclass, only against Defendant Yotta Technologies, Inc.

72. In connection with receiving services, Plaintiff and Class members entered into implied contracts with Yotta.

73. Pursuant to these implied contracts, Plaintiff and Class members paid money to Yotta and provided Yotta with their PII. In exchange, Yotta agreed to, among other things, and Plaintiff understood that Yotta would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards.

74. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Yotta, on the other hand. Had Plaintiff and Class members known that Yotta would not adequately protect its current and former customers' PII, they would not have sought services from Yotta.

75. Plaintiff and Class members performed their obligations under the implied contract when they provided Yotta with their PII and paid for services from Yotta.

76. Yotta breached its obligations under the implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

77. Yotta's breach of its obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

78. Plaintiff and all other Class members were damaged by Yotta's breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. This claim is pleaded in the alternative to the breach of implied contract claim.

81. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to Defendants for services, either directly or indirectly, and through the provision of their PII.

82. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used to facilitate payment.

83. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members

paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

84. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

85. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100 et seq. ("CCPA")

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

88. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he is a "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

89. Defendants are "business[es]" as defined by Civ. Code § 1798.140(c) because each:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in and is headquartered in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

90. Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure because of Defendants' inadequate security measures.

91. Plaintiff's PII was in nonencrypted and nonredacted form, allowing criminals full access to it.

92. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Defendants failed to implement reasonable security procedures to prevent unauthorized access of Plaintiff's and Class members' PII as a result of a cyber-attack.

93. Plaintiff will provide written notice to Defendants pursuant to Civil Code § 1798.150(b), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have or are violating. Although a cure is not possible under the circumstances, if as expected Defendants are unable to cure or do not cure the violation within 30 days of receipt, Plaintiff

will amend this complaint to pursue actual or statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

94. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive and declaratory relief and any other relief as deemed appropriate by the Court.

COUNT VI
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200 et seq. ("UCL")

95. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

96. The California Unfair Competition Law, Bus. & Prof. Code §§ 17200 et seq., prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

97. In the course of conducting their business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the CCPA, Section 5 of the FTCA, and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other

unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

98. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution (California's constitutional right to privacy), and Section 5 of the FTCA. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

99. The UCL also prohibits any "fraudulent business act or practice." Defendants' nondisclosures and misrepresentations regarding the vulnerability of their network systems and their inadequate data security were false, misleading, and likely to deceive the consuming public in violation of the UCL.

100. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of the UCL. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled

to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

101. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate

injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: August 8, 2024

Respectfully submitted,

/s/ Kevin H. Sharp
Kevin H. Sharp, BPR No. 016287
Brent A. Hannafan, BPR No. 025209*
Kristi S. McGregor, GA Bar No. 674012*
SANFORD HEISLER SHARP, LLP
611 Commerce Street, Suite 3100
Nashville, TN 37203
Telephone: (615) 434-7000
Facsimile: (615) 434-7020
ksharp@sanfordheisler.com
bhannafan@sanfordheisler.com
kmcgregor@sanfordheisler.com
**Attorney admission forthcoming*

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
**Pro hac vice forthcoming*

Attorneys for Plaintiff Evin Shefa